UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,602	12/23/2003	Gene Linetsky	VIV/0015.00	1601

28653 7590 06/11/2008

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/707,602
Filing Date: December 23, 2003
Appellant(s): LINETSKY, GENE

John A. Smart
(Reg. No. 34,929)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 03/31/2008 appealing from the Office action mailed on 10/15/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0194486	Heinrich et al.	11-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-58 rejected under 35 U.S.C. 102(e) as being anticipated by Heinrich et al. (Publication Number 2002/0194486) (hereinafter Heinrich).

Regarding claims 1, 23 and 43, Heinrich discloses when a device is first attached to the computer, requiring user-provided information for authorizing the device (Heinrich: paragraphs [0034-0035 and 0045]); based on the user-provided information, storing authorization information indicating that the device is allowed to communicate with the computer (Heinrich: paragraphs [0009, 0015] and 0034-0035); detecting detachment of the device from the computer (Heinrich: see Abstract section and paragraphs 0034-0035); updating the authorization information to indicate that the device is no longer authorized to communicate with the computer (Heinrich: paragraphs [0016-0017 and 0045]); and upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device (Heinrich: paragraphs [0009, 0015 and 0034-0035], the device remains locked until the passwords match).

Regarding claims 2 and 24, Heinrich further discloses specifying a password for authorizing the device (Heinrich: see Abstract section and paragraph [0045]).

Regarding claims 3, 25 and 44, Heinrich further discloses specifying at least one user with sufficient privileges to authorize the device (Heinrich: paragraphs [0034-0035 and 0044-0045]).

Regarding claims 4, 26 and 45, Heinrich further discloses wherein the device is attached to the computer via a port (Heinrich: see figure 1 and paragraphs [0031 and 0037]).

Regarding claims 5 and 27, Heinrich further discloses wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port (Heinrich: paragraphs [0031 and 0037]).

Regarding claims 6, 28 and 46, Heinrich further discloses wherein said device comprises an input device and wherein said blocking step includes blocking input from the input device (Heinrich: paragraphs [0013, 0023 and 0035]).

Regarding claims 7, 29 and 47, Heinrich further discloses wherein said input device is a keyboard device (Heinrich: paragraphs [0015 and 0031]).

Regarding claims 8, 30 and 48, Heinrich further discloses upon reattachment of the keyboard device, trapping keystrokes from the keyboard device (Heinrich: paragraphs [0009 and 0034-0035]).

Regarding claims 9, 31 and 49, Heinrich further discloses determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device (Heinrich: paragraphs [0034-0035]).

Regarding claims 10 and 32, Heinrich further discloses wherein said device comprises a detachable storage device and wherein said blocking step includes blocking any data stream from the storage device (Heinrich: paragraphs [0006 and 0031]).

Regarding claims 11, 33 and 50, Heinrich further discloses wherein said blocking step includes: blocking communication from the computer to the device while the device remains unauthorized (Heinrich: paragraphs [0013, 0023, 0035 and 0045]).

Regarding claims 12 and 34, Heinrich further discloses receiving input authorizing the device; and thereafter allowing communication with the device (Heinrich: paragraphs [0013, 0015 and 0034-0035]).

Regarding claims 13 and 35, Heinrich further discloses wherein the input comprises password input from an authorized user (Heinrich: paragraphs [0034-0035]).

Regarding claims 14, 36 and 51, Heinrich further discloses upon detecting detachment of the device from the computer, generating an alert that reports the detachment (Heinrich: paragraphs [0014, 0016-0017, 0042 and 0044]).

Regarding claims 15, 37 and 52, Heinrich further discloses wherein the alert is automatically transmitted to a system administrator (Heinrich: paragraphs [0013, 0040 and 0044]).

Regarding claims 16, 38 and 53, Heinrich further discloses wherein the alert is automatically transmitted to a remote administration module operating on a different computer (Heinrich: paragraphs [0014, 0016-0017, 0042 and 0044]).

Regarding claims 17, 39 and 54, Heinrich further discloses receiving authorization from a remote administration module; and thereafter allowing communication with the device (Heinrich: paragraphs [0013, 0015 and 0034-0035]).

Regarding claims 18, 40 and 55, Heinrich further discloses wherein said specifying step includes: specifying an operating system hook that allows attachment and detachment of devices to be detected (Heinrich: see Abstract section).

Regarding claims 19, 41, Heinrich further discloses updating the authorization information to indicate that the device is currently untrusted (Heinrich: see Abstract section and paragraph [0045]).

Regarding claims 20, 42 and 56, Heinrich further discloses wherein said updating step includes: treating the detachment as a security breach and blocking communication with a network node that the computer resides on (Heinrich: paragraphs [0013, 0023, 0035 and 0045]).

Regarding claims 21 and 57, Heinrich further discloses a computer-readable medium having processor-executable instructions for performing the method of claim 1 (Heinrich: see figures 1 and 2).

Regarding claims 22 and 58, Heinrich further discloses a downloadable set of processor-executable instructions for performing the method of claim 1 (Heinrich: see Abstract section and paragraphs [0034-0035]).

(10) Response to Argument

In the instant appeal brief, Appellant has the presented the following arguments:

i. Appellant argues as regarding claims 1, 23 and 43 that **Heinrich has no facility to detect attachment events themselves** (i.e., initial attachment, detachment, and reattachment) for peripheral devices.

ii. Appellant argues as regarding claims 1, 23 and 43 that **Heinrich does not cover the scenario where the device is removed, tampered with, and then plug it back into the same slot/same base address**.

iii. Appellant argues as regarding claims 1, 23 and 43 that **Heinrich contains no teaching or suggestion that a given device be authorized by a user at the very outset when it is first attached** (i.e., before it is allowed to interact with the computer system).

iv. Appellant argues as regarding claims 1, 23 and 43 that **Heinrich contains not teaching or suggesting that a given device be reauthorized by a user at each and every subsequent reattachment event** (i.e., regardless of whether the base address for the device has changed).

v. Appellant argues as regarding claims 1, 23 and 43 that **Heinrich certainly has no mechanism where it refuses the initial attachment of an unknown peripheral devices or it refuses reattachment of a known peripheral device to the same slot or port** (until that reattachment is authorized).

As regard to Appellant's first argument, Examiner respectfully disagrees. Heinrich reference teaches a method for securing certain Plug and Play peripheral devices even though those devices are moved (See Abstract section: *identifying information of various Plug and Play ISA devices inserted and re-inserted into slots connected to the ISA bus*). According to the Microsoft Computer Dictionary, the term "Plug and Play" defines as *a set of specifications developed by Intel and Microsoft that allows a PC to configure itself automatically to work with peripherals such as monitors, modems, and printers. A user can plug in a peripheral and "play" it without manually configuring the system*. Heinrich further teaches detecting a change in I/O address and accesses can be prevented by associating the changed I/O address so that it would be of further benefit to disable security of a slot previously occupied by a secured device, but re-assigned to a device that is not to be secured (See paragraphs 0008, 0016-0017, 0020, 0033-0035, 0042 and 0044-0045). When a computer system detects a change in I/O address, Examiner interprets the detection of the I/O change described above as a detection of a device attached, detached or reattached. Therefore, Heinrich does teach detecting attachment events recited in claims 1, 23, and 43.

As regard to Appellant's second argument, Examiner respectfully disagrees. Heinrich teaches a method for keeping track of Plug and play devices inserted and re-inserted (See Abstract section and paragraphs 0008, 0016-0017, and 0022: "*may not remain secured if that peripheral device is reassigned to a dissimilar slot during removal of its associated adapter card and re-insertion of that card into another slot" and "<u>detect a change in I/O address associated with the secured group of peripheral devices</u> and to* *prevent accesses to the secured group of peripheral devices before and after the I/O addresses associated therewith are changed"*). Examiner notes the process of inserted and re-inserted of the Plug and Play devices and the detection of the I/O change (See paragraphs 0017, 0033-0035, 0042 and 0044-0045) recited in Heinrich reference is equivalent to the attachment, detachment and reattachment process recited in claims 1, 23, and 43. Therefore, Heinrich does cover the scenario for removing the device and plugging it back in.

As regard to Appellant's third argument, Examiner respectfully disagrees. Heinrich teaches an authentication process which is used to authenticate a device before the device is allowed to get access to the computer system (See paragraphs 0017 and 0033-0035: *accesses can be prevented by associating the changed I/O address as one that is to remain secured*). Heinrich further teaches If a particular Plug and Play device wants to interact with the computer system, the conductor or slot of that Plug and Play device must be verified (See paragraphs 0033-0035, 0042, and 0044: *the lock signal may be placed upon a specific slot or conductor dedicated to a particular peripheral device. That device will remain locked until the passwords match, thereby preventing read/write data to be presented to that device via masking logic*). Therefore, Heinrich does teach authenticating the device before it is allowed to interact with the computer system recited in Appellant invention.

As regard to Appellant's fourth argument, Examiner respectfully disagrees. Heinrich teaches a security device within the bus interface that will monitor the Plug and play devices inserted and re-inserted (See figure 2, Abstract section and paragraphs

0017, 0020 and 0044: *the security device includes a black box password and compare unit, a configuration control unit, a security control unit, and masking logic which, in combination, shadows base addresses of securable I/O address spaces and grants access to certain securable I/O address spaces depending on the lock and unlock output of the black box*). Therefore Heinrich does teach a given device be reauthorized by a user at each and every subsequent reattachment event.

As regard to Appellant's fifth argument, Examiner respectfully disagrees. Heinrich does teach the mechanism where it refuses the initial attachment of an unknown peripheral devices or it refuses reattachment of a known peripheral device to the same slot or port (See figure 2 and paragraphs 0013, 0015, 0017, 0020, 0023, and 0034-0036: *"If the black box output yields a lock signal, then the masking logic, upon receipt of the lock signal, will block or mask the reading or writing of ISA data" and "prevent accesses to the secured group of peripheral devices before and after the I/O addresses associated therewith are changed"*). Examiner notes the detection of I/O change will lead to preventing accesses to the computer system which is equivalent to refusing the initial attachment of an unknown peripheral devices or refusing reattachment of a known peripheral device to the same slot/port.

Examiner notes a reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v.Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Trang Doan/

Examiner, Art Unit 2131

Conferees:

Christopher Revak

Primary Examiner AU 2131

/Christopher A. Revak/

Primary Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131